Avoiding and Reporting Scams

Scam artists spend every day working on new ways to victimize consumers, which makes it challenging to warn about every possible variation – but most of these schemes work in similar ways, which can help serve as a "red flag" that you have been approached by a con artist or thief.

Nearly every scam is designed to either steal a victim's money or capture to their personal information. Consumers should be extremely cautious in any situation where a stranger is asking for either of those two things. We encourage you to review the following tips to help guard against common scams.

Potential scams can be reported to the Attorney General's Bureau of Consumer Protection by calling out toll-free Consumer Protection Hotline, at 800-441-2555, or using our online Consumer Complaint Form, located in the "Complaints" section of our website.

Suspicious emails can also be reported to the Internet Crime Complaint Center (IC3), which works with state and federal agencies to track and investigate various scams: The IC3 system was created to coordinate investigations with federal and international law enforcement agencies, because the majority of email scams originate from outside the United States. More information is available by visiting the IC3 website at: http://www.ic3.gov/

Financial Scams

Lottery and Sweepstakes offers –

Lottery and sweepstakes scams come in many different forms – some claim that consumers were selected for the prize because their names were entered in an

international drawing, while others are supposedly linked to contests intended to reward consumers for the use of a debit card or credit card.

The stories told by these scam artists come in many different forms, but nearly all of these bogus contests operate in the same way. The “prize notification” typically includes a check for several thousand dollars, which consumers are asked to immediately deposit into their bank account and then wire-transfer a similar amount to the contest operators in order to pay “taxes” and other “fees” necessary to release their larger prize.

The checks that are included in these bogus lottery offers appear authentic and may include watermarks, holograms and other markings intended to enhance their “official” appearance. Despite their appearance, these checks are counterfeit, altered, stolen or otherwise worthless, and consumers who deposit the checks and wire-transfer money will eventually be required to return any missing money to their bank.

Criminals are counting on the fact that victims will find it hard to resist a realistic looking check for several thousand dollars, especially when that check is supposedly the first installment of a much larger prize. They also know that it may take days or weeks before the checks are identified as worthless, by which time the scam artists have already collected their money and moved on to another location.

Consumers should avoid any sort of contest that requires consumers to wire-transfer money in order to release a much larger prize.

Legitimate lotteries withhold all state and federal taxes, along with any other fees, before they distribute the prize winnings, so there’s no need for consumers to ever send money to lottery operators. Additionally, it is extremely unlikely that consumers will win a lottery or sweepstakes that they have not physically entered and federal law prohibits U.S. citizens from participating in foreign lotteries.

Work-at-home employment offers –

Thieves use Internet ads or email messages to circulate bogus employment ads, including offers for high-paying positions as personal assistants, check processors, mystery shoppers and other part-time or work-at-home positions.

They are hoping that the lure of high-paying jobs will convince consumers to respond quickly, without carefully reviewing the offer for warning signs of a scam.

Specific details of bogus job offers can vary, but added that nearly every job-related scam shares common themes:

- They offer “easy money” for doing little or no work.
- You work from home, rather than an office.
- Consumers must respond quickly.
- It is often impossible to meet your employer face-to-face because they “travel” or are “based overseas.”

Corbett noted that at some point during any of these job scams, consumers will be asked to cash checks for their employers and then wire-transfer some of that money. The expensive reality of these scams is that consumers are depositing counterfeit checks and then wire-transferring money to scam artists outside the United States. Victims typically learn they have been scammed when their banks notify them that the checks they have deposited were actually worthless, which may not happen until days or weeks after consumers have electronically transferred money to the thieves behind these schemes.

Other job-related scams may ask consumers to pay up-front fees in order to apply for a position, or may ask consumers to send a copy of their credit report, revealing detailed information about bank accounts, credit cards and other personal data.

“Grandparent” telephone scams –

A new type of aggressive telephone scam is actively targeting older residents, involving calls about family members who have run into difficulties while traveling outside the United States.

Typically, potential victims receive calls from a person claiming to be their grandson or granddaughter, claiming to have been involved in an accident or encountered legal trouble while traveling in Canada. The “grandchild” explains that he does not have insurance on his car and needs several thousand dollars – either to pay for repairs to his own car, to pay for the damage that was done to another vehicle or to pay various fines.

In other cases, the call might come from a scam artists posing as a police officer, requesting money to pay fines for a family member who has been arrested for hunting or fishing without a license, or other violations.

Criminals use fear, sympathy or emotion to convince consumers to quickly send money to a relative who has run into trouble.

Another type of “long distance” scam involves telephone messages left by individuals posing as police or hospital officials, directing victims to call a special number to receive information about a relative who has been hurt in an accident. The phone numbers that consumers are asked to call are often international numbers, though they may appear to be ordinary U.S. phone numbers, resulting in expensive long-distance bills for unsuspecting victims.

Identity Theft / Personal Information Scams

Security Alerts –

Telephone calls, text messages or emails – supposedly from banks or credit card companies – warn consumers that there is a problem with their bank account or credit card, and ask consumers to “confirm” or ‘verify’ their account numbers and passwords.

The sole purpose of these calls and messages is to convince unwary victims to reveal their account numbers and passwords so that thieves can steal money from their bank accounts or make large purchases with their credit cards.

Legitimate businesses will not call consumers or send messages asking them to divulge their entire account number, password or PIN number – so any request for that level of detailed personal information should be a clear warning sign of a scam.

While some businesses may contact consumers to alert them about potential problems with their accounts, they will not ask individuals to reveal all of your account information by phone or email.

If you do receive a message asking for detailed account information, contact your bank or credit card directly – using the customer service hotline printed on your

card or monthly statement – to report the scam attempt and also to verify that your account is secure.

Any consumer who suspects they have accidentally divulged personal information in response to a scam should immediately contact their bank or credit card company to stop any unauthorized withdrawals or charges to their accounts.

Government Notifications –

Scam artists always look for legitimate events that they can use to gain consumers' trust and lend an air of authenticity to their schemes. Bogus notices, claiming to come from government agencies like the IRS or the Census Bureau, are a popular device for identity thieves who are hoping that trusting victims will respond quickly, without taking steps to confirm that the solicitation is legitimate.

The majority of these government-related scams are aimed at getting consumers to divulge detailed personal information, including Social Security numbers, bank account and credit card numbers, or account PIN's and passwords. This information can be used or resold by identity thieves who steal money from victims' bank accounts or make unauthorized purchases using their credit cards.

Many of these schemes will use the lure of refunds, tax credits or government grants to tempt potential victims into responding. Often, these scam messages will include authentic-looking forms or links to Internet sites that resemble actual government sites.

While some phony websites and messages can be easily identified because of spelling errors, poor grammar and other obvious mistakes, but he added that scam artists are growing increasingly sophisticated.

The best way to spot a scam is to understand that legitimate agencies will NOT ask consumers to divulge detailed personal information by email or telephone.

Consumers with questions about suspicious government letters or messages should contact the agency directly – either by visiting the nearest regional office for that agency or by using the telephone directory to identify the official telephone number or toll-free hotline for that agency.

Consumers who suspect they have accidentally divulged personal information in response to a scam should immediately contact their bank or credit card company to stop any unauthorized withdrawals or charges to their accounts.